TOO GOOD TO BE TRUE....

A Column on Consumer Issues
by Attorney General Wayne Stenehjem's
Consumer Protection and Antitrust Division

October 26, 2005

PHARMING

Navigating the ever changing world of the Internet is no simple task. Internet users must watch out for "spam e-mails" (unsolicited junk e-mail), "spoofing" (gaining unauthorized access to computers by using a familiar IP address), "phishing" (using e-mail to gather personal and financial information by deceiving the victim into thinking they are dealing with a reputable company), and now "pharming."

"Pharming" redirects users from legitimate commercial websites to bogus sites. The redirected site looks the same as a genuine site and the browser shows that the victim is at the correct Web site. When the user enters a login name and password, the information is captured by the scam artists. These factors make pharming more serious and more difficult to detect.

"Phishing" attempts to scam people one at a time with an individual e-mail while "pharming" allows a scammer to target large groups of people through domain spoofing. While the tactics used by pharmers have been around for awhile, the rise in Internet banking, online shopping and electronic bill paying has created a wide potential market for criminals eager to snag login information, credit card and bank account numbers. This information can open the door to identity theft.

Identity theft is the fastest growing crime in the United States and involves criminals who obtain information about you that they then use to make purchases or to enter contracts in your name. With a few precautions and a little common sense you can beat these criminals at their own game.

The best way to avoid pharming attacks is to have anti-virus software with up-to-date definitions. Here are other some tips to help prevent "pharming" attacks:

- Be suspicious if you correctly type in a web address and get an error message.
- Use websites of companies that have protection.
- Consider using security programs like Norton Internet Security or Anonymizer that are updated to offer protection from pharming scams.
- Consider using adware/spyware detector and removal programs.
- Ensure that security patches and antivirus software are updated regularly.

Here are more general tips to help prevent your personal and financial information from being stolen via Internet scammers:

- It is very rare for a bank or business to ask for your account details. If you get such a request, call and check first before providing the requested information.
- If you don't know the source the e-mail is likely to be bogus. Check it against previous correspondence if you are unsure.
- If you get a request for urgent action don't jump to it. Stop, think, and double-check with the institution before acting.
- Look at website addresses on your browser. If you are supposed to be on a secure site, the start of the address should be https:// rather than just http://. Check 'Properties' from the file menu to display more information.
- Look at the page layout and design. Company logos are easy to copy from the Internet, but if the site looks different from normal, call the company and check.

If you are not sure about an e-mail or a website, ASK QUESTIONS. Know who and what you are dealing with before completing an Internet inquiry or transaction.

The Attorney General's Consumer Protection Division investigates allegations of fraud in the marketplace. Investigators also mediate individual complaints against businesses. If you have a consumer problem or question, call the Consumer Protection Division at 328-3404, toll-free at 1-800-472-2600, or 1-800-366-6888 (w/TTY). This article and other consumer information is located on our website at www.ag.state.nd.us.

* * * * *